CORRESPONDS TO JP2003-531062

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
2. August 2001 (02.08.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/55836 A1

(51) Internationale Patentklassifikation⁷: G06F 7/58

(21) Internationales Aktenzeichen: PCT/DE01/00111

(22) Internationales Anmeldedatum:
12. Januar 2001 (12.01.2001)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
100 03 472.1 27. Januar 2000 (27.01.2000) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: INFINEON TECHNOLOGIES AG [DE/DE]; St.-Martin-Strasse 53, 81669 München (DE).

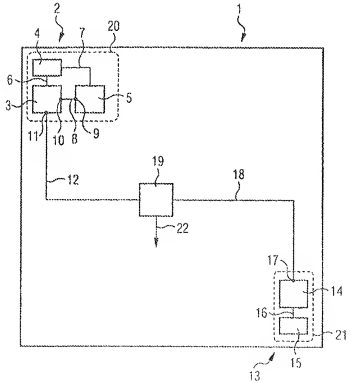
(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: JANSSEN, Norbert [DE/DE]; Innere Wiener Strasse 13A, 81667 München (DE).

(74) Anwalt: EPPING HERMANN & FISCHER; Postfach 12 10 26, 80034 München (DE).

[Fortsetzung auf der nächsten Seite]

(54) Title: RANDOM NUMBER GENERATOR

(54) Bezeichnung: ZUFALLSZAHLENGENERATOR



(57) Abstract: The invention relates to a random number generator on an integrated circuit (1), comprising a first clock generator circuit (2) with a first voltage supply (4), for producing a first signal with a first frequency or a first frequency range; a second clock generator circuit (13) with a second voltage supply (15), for producing a second signal with a second frequency or a second frequency range which is or whose average is lower than the first frequency; and a generator (19) in which the first signal can be sampled with the second signal and which can generate a random number according to the sampling result. The invention is characterized in that the clock generator circuits (2, 13) are situated as far apart as possible from each other on the integrated circuit (1) and/or the two voltage supplies (4, 15) are separated from each other and/or at least one guard ring (20, 21) is placed around each of the clock generator circuits (2, 13).

(57) Zusammenfassung: Die Erfindung ist gerichtet auf einen Zufallszahlengenerator auf einem integrierten Schaltkreis (1) mit einer ersten Taktgeberschaltung (2) mit einer ersten Spannungsversorgung (4) zur Erzeugung eines ersten Signals einer ersten Frequenz oder eines ersten Frequenzbereichs;

[Fortsetzung auf der nächsten Seite]

WO 01/55836 A1

(81) Bestimmungsstaaten *(national)*: BR, CA, CN, IL, IN, JP, KR, MX, RU, UA, US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Veröffentlicht:
— *mit internationalem Recherchenbericht*
— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

einer zweiten Taktgeberschaltung (13) mit einer zweiten Spannungsversorgung (15) zur Erzeugung eines zweiten Signals einer zweiten Frequenz oder eines zweiten Frequenzbereichs, die oder dessen Mittelwert niedriger als die erste Frequenz ist; und einem Generator (19), in dem das erste Signal vom zweiten Signal abtastbar ist und der in Abhängigkeit vom Ergebnis der Abtastung zumindest eine Zufallszahl erzeugen kann. Die Erfindung ist dadurch gekennzeichnet, dass die Taktgeberschaltungen (2, 13) auf dem integrierten Schaltkreis (1) möglichst weit voneinander entfernt angeordnet sind und/oder die beiden Spannungsversorgungen (4, 15) voneinander getrennt sind und/oder um jede der Taktgeberschaltungen (2, 13) zumindest ein Guardring (20, 21) gelegt ist.

Beschreibung

Zufallszahlengenerator

Die vorliegende Erfindung betrifft eine Schaltungsanordnung zur Erzeugung von Zufallszahlen, insbesondere die Anordnung der Schaltung für einen Zufallszahlengenerator auf einem integrierten Schaltkreis.

Die Erzeugung von Zufallszahlen ist für viele Gebiete der Wissenschaft und Technik von großer Bedeutung. So werden Zufallszahlen für zahlreiche Anwendungen in der Statistik ebenso benötigt wie für kryptographische Zwecke. Gerade die Kryptographie gewinnt im Zuge der Ausbreitung von Datennetzen und der damit verbundenen Sicherheitsproblematik zunehmend an Bedeutung. Daher stellt die automatische Erzeugung von Zufallszahlen ein wichtiges Gebiet der Elektrik und Elektronik, speziell der Datenverarbeitung, dar. Wichtig ist nicht nur die Erzeugung von Zufallszahlen, sondern auch deren Qualität. Nicht mit allen Verfahren lassen sich Zufallszahlen generieren, welche gleich "zufällig" sind. Vielmehr lassen sich meist, gerade bei Analyse einer großen Zahl von Zufallszahlen, welche ein bestimmter Zufallszahlengenerator erzeugt hat, Muster erkennen, die zu einer Abweichung von der idealen, zufälligen Verteilung der erzeugten Zahlen führen. Ein Maß für die Qualität von Zufallszahlen ist ihre Entropie, wie von Shannon in "A Mathematical Theory of Communication", The Bell System Technical Journal, Bd. 27, S. 379 (1948) beschrieben.

Ein im Stand der Technik bekanntes Verfahren zur Erzeugung von Zufallszahlen besteht in der Abtastung eines Signals mit hoher Frequenz durch ein zweites Signal mit wesentlich niedrigerer Frequenz. Bei diesen Signalen handelt es sich also um an bestimmten Ausgängen anliegende Spannungen, die zwischen zwei Amplitudenwerten hin und her oszillieren und dies im zeitlichen Verlauf mit einer bestimmten Geschwindigkeit tun.

Die Abtastung erfolgt in einem speziellen Schaltkreis, in den beide Signale eingespeist werden. Hierbei wird stets ein bestimmter Punkt im Wellenverlauf des zweiten Signals verwendet, um einen Zeitpunkt zu bestimmen, zu dem das erste Signal abgetastet, das heißt der Wert des Signals (beispielsweise gemessen als Spannung) festgestellt und in einen numerischen Wert umgesetzt wird.

Bei Digitalschaltungen sind dies im einfachsten Fall die Werte Null oder Eins, beispielsweise wenn sich zum Zeitpunkt der Abtastung der Wellengang des ersten Signals oberhalb des Mittelwerts (beispielsweise 0 Volt) befindet als "Eins", und wenn sich der Wellengang unterhalb des Mittelwerts befindet, als "Null". Es ist jedoch genau so möglich, eine kontinuierliche Interpretation des erhaltenen Werts zu machen, um somit eine Analogzahl zu erhalten (beispielsweise eine Spannung in Millivolt, die 1:1 als Zahl umgesetzt wird).

Bei idealen Wellengängen der beiden Signale würde eine Periodizität bei der Abtastung der Amplitudenwerte zu beobachten sein, die sich aus dem Verhältnis der beiden Frequenzen ergibt. Somit wäre es nicht möglich, echte Zufallszahlen mit Hilfe eines solchen Zufallszahlengenerators zu erzeugen. In der Praxis handelt es sich bei den Wellen der beiden Signale jedoch nicht um ideale Wellengänge, sondern es wird, gerade im mikroelektronischem Bereich, durch ein unvermeidbares Rauschen eine Ungenauigkeit im Wellengang erzeugt. Dies kann dazu führen, daß bereits mit zwei einfachen vorgegebenen Frequenzen ein gut funktionierender Zufallszahlengenerator erreicht werden könnte, wenn die Signale voneinander unabhängig wären.

In der Praxis genügt jedoch ein solch einfacher Zufallszahlengenerator nicht den hohen Anforderungen an die Qualität der zu erzeugenden Zufallszahl. Von wesentlicher Bedeutung für die Qualität der Zufallszahlen ist dabei nämlich, daß die beiden Signale voneinander unabhängig sind. Dies bedeutet,

daß nicht das eine Signal durch in der verwendeten Schaltung befindliche elektrische Signalwege zu einer Beeinflussung des anderen Signals führt, so daß die beiden Signale in einer bestimmten Art und Weise miteinander gekoppelt sind.

Bei sogenannten physikalischen Rauschgeneratoren, die dem obigen Prinzip entsprechen, versucht man dieses Problem der Unabhängigkeit der beiden Signale beispielsweise dadurch zu lösen, daß das abzutastende Signal, also das erste Signal, eine nicht konstante Frequenz hat. Ein solches abzutastendes Signal kann man beispielsweise erhalten, indem in die Schaltung zur Erzeugung der Zufallszahlen ein sogenannter spannungsgekoppelter Oszillator (voltage controlled oscillator, VCO) integriert wird, dessen Steuereingang von einem periodisch sich verändernden Signal, wie es beispielsweise ein zweiter Oszillator bereitstellt, gespeist wird. Im Ergebnis führt dies dazu, daß in Abhängigkeit von dem Wellengang des zweiten Oszillators die Frequenz des Signals des VCOs moduliert wird. Der zweite Oszillator kann hierbei auch ein VCO sein, der beispielsweise an seinem Steuereingang mit einer konstanten Spannung betrieben wird, so daß an seinem Signalausgang ein Schwingungssignal konstanter Frequenz ausgegeben wird. Auch dieser Ansatz hat jedoch noch nicht zu für alle Einsatzgebiete befriedigenden Ergebnissen geführt. Im Ergebnis kann es vorkommen, daß die beiden Signale zeitweilig gekoppelt werden, so daß sich eine Mischfrequenz bildet, sofern die Frequenz des ersten Signals zu einem bestimmten Zeitpunkt für eine solche Kopplung geeignet ist und die beiden Signale nach einer bestimmten Zeit wieder auseinanderfallen. Dadurch schwankt die Qualität der von der Schaltung bereitgestellten Zufallszahlen mit der sich verändernden Frequenz des ersten Signals. Es besteht somit weiterhin Bedarf an Zufallszahlengeneratoren, bei denen die Qualität der erzeugten Zufallszahlen besser ist.

In der DD 279 763 A1 ist ein Verfahren zur Erzeugung von Zufallszahlen in Mikrorechnern beschrieben, bei dem zwei nicht-

korrelierte elektrische Schwingungen genutzt werden, deren Frequenzen sich mindestens um den Faktor 100 unterscheiden. Die Schwingungen werden von zwei unabhängigen Quellen erzeugt, und zwar derart, dass weder zwischen den Frequenzen noch zwischen den Phasenlagen der beiden Schwingungen eine Korrelation besteht. Die Schwingungen der höheren Frequenz werden von einem Zähler gezählt, der durch einen Mikrorechner gestartet wird, und die Schwingung der niedrigeren Frequenz wird zum Stoppen des Zählers genutzt. Die Zufallszahl steht dann nach dem Stoppen des Zählers als Zählerstand zur weiteren Verarbeitung zur Verfügung.

In der US 5,859,540 ist ein Guard-Ring beschrieben, der zur Verringerung des Dunkelstroms einer Fotodiode vorgesehen ist. Es handelt sich dabei um einen ringförmigen hoch dotierten Bereich in Halbleitermaterial, der gemäß der Beschreibung in Spalte 4 die Lage der Verarmungszone verändert und so den Dunkelstrom reduziert. Ein Guard-Ring ist allgemein ein dotierter Bereich in Halbleitermaterial, der ein Bauelement zum Zweck der Stromeingrenzung umgibt.

Der vorliegenden Erfindung liegt damit die Aufgabe zugrunde, einen gattungsgemäßen Zufallszahlengenerator bereitzustellen, bei dem Unabhängigkeit der beiden Signale besser gewährleistet ist als bislang vorbekannt. Diese Aufgabe löst der Zufallszahlengenerator gemäß dem unabhängigen Patenanspruch 1. Weitere vorteilhafte Ausgestaltungen, Aspekte und Details der Erfindung ergeben sich aus den abhängigen Patentansprüchen, der Beschreibung und den beigefügten Zeichnungen.

Der vorliegenden Erfindung liegt das Prinzip zugrunde, eine Reihe von Maßnahmen bereitzustellen, die einzeln oder in Kombination die Unabhängigkeit der beiden Signale des Zufallszahlengenerator entscheidend verbessern können.

Die Erfindung ist daher allgemein gerichtet auf einen Zufallszahlengenerator auf einem integrierten Schaltkreis mit

einer ersten Taktgeberschaltung, mit einer ersten Spannungsversorgung zur Erzeugung eines ersten Signals einer ersten Frequenz oder eines ersten Frequenzbereichs, einer zweiten Taktgeberschaltung mit einer zweiten Spannungsversorgung zur Erzeugung eines zweiten Signals einer zweiten Frequenz und eines zweiten Frequenzbereichs, die oder dessen Mittelwert niedriger als die erste Frequenz ist und einen Generator, in dem das erste Signal vom zweiten Signal abtastbar ist und der in Abhängigkeit vom Ergebnis der Abtastung zumindest eine Zufallszahl erzeugen kann, dadurch gekennzeichnet, daß die Taktgeberschaltungen auf dem integrierten Schaltkreis möglichst weit voneinander entfernt angeordnet sind und/oder die beiden Spannungsversorgungen voneinander getrennt sind und/oder um jede der Taktgeberschaltungen zumindest ein Guardring gelegt ist.

Die erste Taktgeberschaltung, welche das abzutastende Signal liefert, kann also entweder eine feste Frequenz erzeugen oder eine variable Frequenz ausgeben, die in einem vorgehenden Frequenzbereich variiert. Der einfachste Fall einer festen Frequenz ist bereits oben als Stand der Technik beschrieben worden und basiert auf dem Prinzip, daß durch unvermeidbares Rauschen innerhalb der Bauelemente dennoch Zufallszahlen erzeugt werden können. Die Verwendung eines kompletten Frequenzbereichs, also die Ausgabe eines Signals variabler Frequenz, ist aktueller Stand der Technik.

Das gleiche gilt für die zweite Taktgeberschaltung. Während diese üblicherweise von fixer Frequenz ist, kann es genauso möglich sein, auch das zweite Signal von variabler Frequenz mit einem bestimmten Frequenzbereich zu gestalten. In diesem Fall kann die Anzahl der erzeugten Zufallszahlen pro Zeiteinheit mit der Frequenz des zweiten Signals schwanken. Diese Ausgestaltung kann allerdings den Vorteil haben, die Qualität der Zufallszahlen zu verbessern.

Wie oben geschildert, erzeugt der Generator Zufallszahlen durch Auswertung der zeitlichen Verläufe und Werte der beiden Signale. Im einfachsten Fall kann der Generator ein FlipFlop sein, in dessen Eingang das erste Signal eingespeist wird und dessen Ausgang stets dann mit einem neuen Wert beschaltet wird, wenn beispielsweise das zweite Signal, das an einem Steuereingang anliegt, eine aufsteigende Flanke hat. Entsprechende Realisierungen einer solchen Schaltung sind dem Fachmann geläufig.

Die Entfernung der beiden Taktgeberschaltungen auf dem integrierten Schaltkreis bis zum maximal Möglichen führt dazu, daß die Beeinflussung der beiden Signale aufeinander mit der Entfernung abnimmt. In Abhängigkeit von der Größe des gesamten integrierten Schaltkreises kann man hiermit ein unterschiedlich gutes Resultat erzielen. Unter "möglichst weit voneinander entfernt" ist hierbei zu verstehen, daß der Abstand der Komponenten, welche die beiden Taktgeberschaltungen bilden, unter Berücksichtigung sonstiger schaltungstechnischer Gegebenheiten des integrierten Schaltkreises in einem denkbar großen Abstand voneinander liegen, beispielsweise in diagonal entgegengesetzten Ecken des integrierten Schaltkreises.

Die erfindungsgemäße Trennung der Spannungsversorgungen führt dazu, daß das Signal kein Übersprechverhalten auf die elektrischen Ströme der Spannungsversorgung bewirken kann, was einen üblichen Weg zur Koppelung der Frequenzen der beiden Signale darstellt.

Guardringe schließlich helfen ebenfalls, die Ausbreitung der Signale über den integrierten Schaltkreis zu verhindern.

Insbesondere wird bevorzugt, daß zwei oder sogar alle drei der vorgeschlagenen Maßnahmen bei einem Zufallszahlengenerator auf einem integrierten Schaltkreis gemäß der vorliegenden

Erfindung gleichzeitig realisiert sind. Alle Maßnahmen tragen dazu bei, die Unabhängigkeit der Signale zu verbessern.

Die Trennung der Spannungsversorgungen kann vorzugsweise durch zumindest ein RC-Glied erfolgen. RC-Glieder sind Baugruppen, welche nur Signale in einen bestimmten engen Frequenzbereich passieren lassen und andere Frequenzen sperren. Somit kann ein RC-Glied ausgewählt werden, welches das andere Signal, welches ja eine andere Frequenz hat, effektiv am Eintritt in die jeweils andere Taktgeberschaltung hindern kann. Es ist auch möglich, das RC-Glied so zu bemessen, daß es den Austritt des Signals aus der Taktgeberschaltung verhindert. Wenn die ausgegebene Frequenz eine variable Frequenz ist, bietet es sich an, das RC-Glied so auszuwählen, daß der Mittelwert der vorhandenen Frequenzen durchgelassen wird. Während es hinreichend sein kann, ein RC-Glied zu verwenden, das eine der Spannungsversorgungen filtert, kann vorzugsweise für jede der Taktgeberschaltungen jeweils ein RC-Glied vorgesehen sein, welches diese abtrennt.

Alternativ oder zusätzlich zur Verwendung von RC-Gliedern kann es auch möglich sein, die Trennung der Spannungsversorgungen durch zumindest einen Spannungsregler zu bewirken. Hierbei können also beide Taktgeberschaltungen zunächst von einer gemeinsamen Spannungsversorgung versorgt werden, wobei jedoch diese über jeweils einen Spannungsregler geführt wird, der bauartbedingt ebenfalls eine Trennung der Signale ermöglicht.

Die Erfindung kann dadurch gekennzeichnet sein, daß das erste Signal eine variable Frequenz aufweist, oder dadurch, daß das zweite Signal eine variable Frequenz aufweist. Wie bereits oben erläutert, bezieht sich dies auf die Möglichkeit, durch Verwendung von entsprechenden Bauteilen, die Frequenz sich periodisch ändern zu lassen.

Wie bereits bei der Erläuterung des Stands der Technik ausgeführt, ist es vorteilhaft, daß die Frequenz des zweiten Signals wesentlich niedriger ist als die Frequenz des ersten Signals. Insbesondere wird es bevorzugt, daß das zweite Signal eine Frequenz hat, die zumindest zehnmal niedriger ist als die Frequenz des ersten Signals, besonders bevorzugt zumindest einhundertmal niedriger als die Frequenz des ersten Signals.

Die Auswahl der Frequenzen erlaubt es, einen sogenannten Jitter (Variation des zeitlichen Auftretens eines bestimmten Signalzustands) für das zweite Signal zu erhalten, welcher mehrere Schwingungen des ersten Signals überdeckt, so daß eine zufälligere Abtastung des ersten Signals möglich ist.

Der Generator erzeugt zumindest eine Zufallszahl. Da jedoch die Taktgeberschaltungen ein kontinuierliches Signal liefern, bietet es sich an und wird bevorzugt, daß der Generator eine Abfolge von Zufallszahlen erzeugt. In der Tat wird in aller Regel ein Strom von Zufallszahlen erzeugt, der in Abhängigkeit von dem Erreichen eines bestimmten Bereichs im Wellengang des zweiten Signals jeweils eine Zahl, beziehungsweise eine Ziffer einer Zahl, liefert. Beispielsweise ist es möglich, den Generator so auszulegen, daß er Binärzahlen erzeugt, die aus Nullen und Einsen bestehen, und jeweils eine vorbestimmte Zahl dieser Binärwerte zu einer Gesamtzufallszahl zusammenzufassen. So ist es beispielsweise möglich, 16 oder 32 Binärzahlen zu einer geeigneten Zufallszahl von 16 bzw. 32 Bit zusammenzufassen.

Wie bereits ausgeführt, kann der Generator in einer einfachen Ausführungsform aus lediglich einem FlipFlop bestehen. Dies kann jedoch trotz der erfindungsgemäßen Maßnahmen dazu führen, daß der Generator, z.B. wegen der nichtkonstanten Frequenz des zweiten Signals, eine nicht konstante Leistung bei der Zufallszahlenerzeugung erbringt. Weiterhin kann die Zufallszahl zu einem bestimmten Wert hin beeinflußt sein, also

eine inhärente Gewichtung haben. Es wird daher bevorzugt, daß der Generator weiterhin aufweist eine Ausgleichsschaltung zur Kompensation einer nicht konstanten Leistung und/oder einer Gewichtung bei der Zufallszahlenerzeugung. Hat auch das zweite Signal, welches das erste Signal abtastet, einen schwebenden Verlauf (d.h. eine sich zwischen einem minimalen und einem maximalen Wert periodisch ändernde Frequenz), so ändert sich auch die Leistung des Zufallszahlengenerators mit der Freuqenz. Dies lässt sich durch eine bevorzugte Ausgleichsschaltung kompensieren, welche sich beispielsweise durch ein rückgekoppeltes Schieberegister realisieren lässt, welchem die Ausgangssignale des Zufallszahlengenerators zugeführt werden. Bekanntermaßen ist ein Schieberegister ein Entropiespeicher. Entnimmt man dem Schieberegister mit einer konstanten Rate, welche kleiner oder gleich der minimalen Ausgangssignalrate des Zufallszahlengenerators ist, Signale, beispielsweise Bits, so hat der entnommene Signalstrom (beispielweise ein Bitstrom) eine Entropie, die größer oder gleich der Entropie des Signalstroms aus dem Zufallszahlengenerator ist. Es sind jedoch auch andere Nachbearbeitungsverfahren an Schaltungen vorstellbar, welche dazu dienen, die Qualität der erzeugten Zufallszahlen zu verbessern.

In weiteren bevorzugten Ausführungsformen kann die erste und/oder die zweite Taktgeberschaltung zumindest einen spannungsgekoppelten Oszillator und einen weiteren Oszillator aufweisen, dessen Signalausgang mit einem Steuereingang des spannungsgekoppelten Oszillators verbunden ist. Diese grundsätzlich, wenn auch nicht in Kombination mit der Erfindung, bekannte Anordnung ermöglicht eine weitere Verbesserung der Qualität der Zufallszahlen. Auch der weitere Oszillator kann ein spannungsgekoppelter Oszillator sein, dessen Steuereingang mit einer konstanten Spannung geschaltet ist. Auf diese Weise wirkt der spannungsgekoppelte Oszillator wie ein einfacher Oszillator, der lediglich eine Frequenz abgibt. Bei der Verwendung eines spannungsgekoppelten Oszillators läßt sich

die Schaltung insgesamt vereinfachen, da weniger unterschiedliche Bauteile beziehungsweise Baugruppen, benötigt werden.

Um die Qualität der erzeugten Zufallszahlen weiter zu verbessern, kann es ebenfalls bevorzugt sein, daß die erste und/oder die zweite Taktgeberschaltung eine Mehrzahl von in Reihe geschalteten spannungsgekoppelten Oszillatoren aufweist, wobei der Signalausgang jedes der spannungsgekoppelten Oszillatoren bis auf den letzten der Reihe mit dem Steuereingang des nächsten spannungsgekoppelten Oszillators verbunden ist. Auf diese Weise läßt sich ein noch komplexeres Frequenzmuster bei dem ausgegebenen ersten Signal erzielen, so daß die Periodizität der Abtastung mit dem zweiten Signal weiter wächst.

Im folgenden sollen konkrete Ausführungsbeispiele der vorliegenden Erfindung beschrieben werden, wobei auf die beigefügten Zeichnungen Bezug genommen wird, in denen folgendes dargestellt ist:

Figur 1 zeigt einen Zufallszahlengenerator mit zwei Taktgeberschaltungen in einer einfacheren Ausführungsform der vorliegenden Erfindung; und
Figur 2 zeigt eine komplexere Taktgeberschaltungsanordnung gemäß der vorliegenden Erfindung.

Figur 1 zeigt allgemein einen integrierten Schaltkreis 1 mit einer ersten Taktgeberschaltung 2 und einer zweiten Taktgeberschaltung 13. Die erste Taktgeberschaltung 2 weist einen Taktgeber 3 für das erste Signal und eine Spannungsversorgung 4 für den ersten Taktgeber auf. In diesem Beispiel soll die von der ersten Taktgeberschaltung 2 erzeugte Frequenz des ersten Signals variabel sein, so daß der Taktgeber 3 für das erste Signal beispielsweise ein VCO ist, an dessen Steuereingang 10 ein Zusatzoszillator 5 der ersten Taktgeberschaltung 2 angeschlossen ist, der über den Signalausgang 9 und die Si-

gnalleitung 8 diesen Steuereingang 10 mit einem Signal konstanter Frequenz versorgt.

Die zweite Taktgeberschaltung 13 weist einen Taktgeber 14 für das zweite Signal auf, der im vorliegenden einfacheren Ausführungsbeispiel beispielsweise ein Oszillator konstanter Frequenz sein kann. Dieser wird über die Spannungsversorgung 15 für den zweiten Taktgeber und die Spannungsversorgungsleitung 16 mit einer geeigneten Betriebsspannung versorgt. Die erste Taktgeberschaltung 2 gibt über einen Signalausgang 11 für das erste Signal das Signal aus, welches über eine Signalleitung 12 für das erste Signal dem Zufallszahlengenerator zugeführt wird. Der Taktgeber 14 für das zweite Signal gibt über einen Signalausgang 17 für das zweite Signal und eine Signalleitung 18 das zweite Signal ebenfalls an den Zufallszahlengenerator 19 aus. Nach Erzeugung von Zufallszahlen gibt der Zufallszahlengenerator 19 über die Zufallszahlenausgabe 22 Zufallszahlen aus.

Die erste Taktgeberschaltung 2 weist darüber hinaus eine Spannungsversorgung 4 auf, welche über Spannungsversorgungsleitungen 6, 7 die Taktgeber mit Energie versorgen. Bei der zweiten Taktgeberschaltung 13 ist eine zweite Spannungsversorgung vorgesehen, die über die Spannungsversorgungsleitung 16 den Taktgeber 14 mit Energie versorgt.

Erfindungsgemäß sind die beiden Taktgeberschaltungen 2 und 13 voneinander so weit als möglich beabstandet auf dem integrierten Schaltkreis 1 angeordnet. Dies ist dadurch sichergestellt, daß die entsprechenden Baugruppen in diagonal entgegengesetzte Ecken des integrierten Schaltkreises gelegt worden sind. Falls technisch nicht anders möglich, können jedoch auch andere Orte für die Anordnung der Taktgeberschaltungen verwendet werden.

Desweiteren ist ein erfindungsgemäßer Guardring um jede der beiden Taktgeberschaltungen gelegt. Um die Taktgeberschaltung

2 für das erste Signal ist im folgenden Beispiel ein p-dotierter oder ein N-dotierter Guardring 20 gelegt, während um die zweite Taktgeberschaltung 13 ein gleichdotierter Guardring 21 gelegt ist.

Schließlich können erfindungsgemäß die beiden Spannungsversorgungen 4 und 15 voneinander durch die oben erläuterten Maßnahmen getrennt werden (nicht dargestellt).

Figur 2 zeigt ein komplexeres Ausführungsbeispiel der vorliegenden Erfindung. Die erste Taktgeberschaltung 2 weist hierbei insgesamt drei VCOs auf, nämlich den Taktgeber für das erste Signal 3, den zweiten VCO 23 für das erste Signal und den dritten VCO 24 für das erste Signal, welche alle über die Spannungsversorgungsleitung 6, 7 von der Spannungsversorgung 4 mit Spannung versorgt werden.

Der dritte VCO 24 gibt über einen Signalausgang 30 des dritten VCOs 24 und eine Signalleitung 29 ein Signal konstanter Frequenz an den Steuereingang 31 des zweiten VCOs 23 ab, welcher daraufhin am Signalausgang 9 ein Signal variabler Frequenz über die Signalleitung 8 an den Steuereingang 10 des ersten Taktgebers 3 ausgibt. Dieser erzeugt damit ein komplexeres Signal, das wie oben beschrieben an den Zufallszahlengenerator 19 weitergegeben wird. Die gleiche Anordnung wird im vorliegenden Ausführungsbeispiel auch für die Erzeugung des zweiten Signals verwendet. Hier werden die drei VCOs 25, 26 und 27 verwendet, welche über die Spannungsversorgungsleitung 16 und 28 energieversorgt werden.

Der erfindungsgemäß angeordnete Zufallszahlengenerator ermöglicht die Erzeugung von Zufallszahlen von erheblich besserer Qualität als dies mit vorbekannten Schaltungen möglich war. Die überraschende Einfachheit der vorgeschlagenen Lösungen ermöglicht eine preisgünstigere Realisierung bei der konkreten Implementation von erfindungsgemäßen Zufallszahlengeneratoren.

Patentansprüche

1. Zufallszahlengenerator auf einem integrierten Schaltkreis (1) mit

einer ersten Taktgeberschaltung (2) mit einer ersten Spannungsversorgung (4) zur Erzeugung eines ersten Signals einer ersten Frequenz oder eines ersten Frequenzbereichs;

einer zweiten Taktgeberschaltung (13) mit einer zweiten Spannungsversorgung (15) zur Erzeugung eines zweiten Signals einer zweiten Frequenz oder eines zweiten Frequenzbereichs, die oder dessen Mittelwert niedriger als die erste Frequenz ist; und

einem Generator (19), in dem das erste Signal vom zweiten Signal abtastbar ist und der in Abhängigkeit vom Ergebnis der Abtastung zumindest eine Zufallszahl erzeugen kann;

dadurch gekennzeichnet, daß die Taktgeberschaltungen (2, 13) auf dem integrierten Schaltkreis (1) möglichst weit voneinander entfernt angeordnet sind und/oder die beiden Spannungsversorgungen (4, 15) voneinander getrennt sind und/oder um jede der Taktgeberschaltungen (2, 13) zumindest ein Guardring (20, 21) gelegt ist.

2. Zufallszahlengenerator nach Anspruch 1, dadurch gekennzeichnet, daß die Taktgeberschaltungen (2, 13) auf dem integrierten Schaltkreis (1) möglichst weit voneinander entfernt angeordnet sind und die beiden Spannungsversorgungen (4, 15) voneinander getrennt sind und um jede der Taktgeberschaltungen (2, 13) zumindest ein Guardring (20, 21) gelegt ist.

3. Zufallszahlengenerator nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Taktgeberschaltungen auf dem integrierten Schaltkreis in einander diagonal gegenüberliegenden Eckbereichen des integrierten Schaltkreises (1) angeordnet sind.

4. Zufallszahlengenerator nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die Trennung der Spannungsversorgungen (4, 15) durch zumindest ein RC-Glied erfolgt.

5. Zufallszahlengenerator nach Anspruch 4, dadurch gekennzeichnet, daß beide Spannungsversorgungen (4, 15) durch jeweils ein RC-Glied getrennt sind.

6. Zufallszahlengenerator nach Anspruch 4 oder 5, dadurch gekennzeichnet, daß eine Entkoppelungsfrequenz des eine der Taktgeberschaltungen (2, 13) abtrennenden RC-Glieds dem Mittelwert des Frequenzbereichs des Signals der jeweiligen oder der anderen Taktgeberschaltung (2, 13) entspricht.

7. Zufallszahlengenerator nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Trennung der Spannungsversorgungen (4, 15) durch zumindest einen Spannungsregler erfolgt.

8. Zufallszahlengenerator nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß das erste Signal eine variable Frequenz aufweist.

9. Zufallszahlengenerator nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß das zweite Signal eine variable Frequenz aufweist.

10. Zufallszahlengenerator nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß das zweite Signal eine Frequenz hat, die zumindest zehnmal niedriger ist als die Frequenz des ersten Signals.

11. Zufallszahlengenerator nach Anspruch 10, dadurch gekennzeichnet, daß das zweite Signal eine Frequenz hat, die zumindest einhundertmal niedriger ist als die Frequenz des ersten Signals.

12. Zufallszahlengenerator nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, daß der Generator (19) eine Abfolge von Zufallszahlen erzeugt.

13. Zufallszahlengenerator nach einem der Ansprüche 1 bis 12, dadurch gekennzeichnet, daß der Generator (19) weiterhin aufweist eine Ausgleichsschaltung (32) zur Kompensation einer nichtkonstanten Leistung und/oder einer Gewichtung bei der Zufallszahlenerzeugung.

14. Zufallszahlengenerator nach Anspruch 13, dadurch gekennzeichnet, daß die Ausgleichsschaltung (32) ein linear rückgekoppeltes Schieberegister aufweist.

15. Zufallszahlengenerator nach einem der Ansprüche 1 bis 14, dadurch gekennzeichnet, daß die erste und/oder die zweite Taktgeberschaltung (2, 13) zumindest einen spannungsgekoppelten Oszillator (3, 23, 25, 26) und einen weiteren Oszillator (5, 24, 27) aufweist, dessen Signalausgang (9) mit einem Steuereingang (10) des spannungsgekoppelten Oszillators (3, 23, 25, 26)verbunden ist.

16. Zufallszahlengenerator nach einem Anspruch 15, dadurch gekennzeichnet, daß der weitere Oszillator ein spannungsgekoppelter Oszillator (23, 24, 26, 27) ist, dessen Steuereingang mit einer konstanten Spannung beschaltet ist.

17. Zufallszahlengenerator nach Anspruch 15 oder 16, dadurch gekennzeichnet, daß die erste und/oder die zweite Taktgeberschaltung eine Mehrzahl von in Reihe geschalteten spannungsgekoppelten Oszillatoren aufweist, wobei der Signalausgang jedes der spannungsgekoppelten Oszillatoren bis auf den letzten der Reihe mit dem Steuereingang des nächsten spannungsgekoppelten Oszillators verbunden ist.

FIG 1

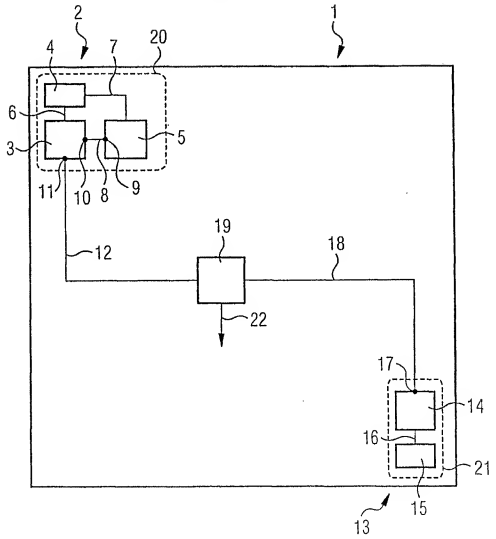
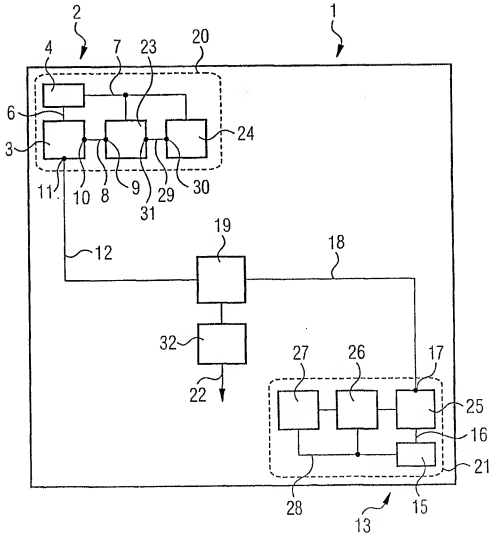


FIG 2


2
1
4
7
23
20
6
3
24
11
10
8
9
29
30
31
19
18
12
32
22
27
26
17
25
16
21
28
15
13

INTERNATIONAL SEARCH REPORT

International Application No
PCT/L_ 01/00111

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"INTEGRATED CIRCUIT COMPATIBLE RANDOM NUMBER GENERATOR" IBM TECHNICAL DISCLOSURE BULLETIN,US,IBM CORP. NEW YORK, vol. 30, no. 11, 1 April 1988 (1988-04-01), pages 333-335, XP000021682 ISSN: 0018-8689 page 334, paragraph 2	1-17
Y	DD 279 763 A (THAELMANN SCHWERMASCHBAU VEB) 13 June 1990 (1990-06-13) cited in the application the whole document	1-17

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 June 2001	04/07/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Cohen, B

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	MURRY: "A General Approach for Generating Natural Random Variables" IEEE TRANSACTIONS ON ELECTRONIC COMPUTERS., vol. c-19, no. 12, December 1970 (1970-12), pages 1210-1213, XP002169916 IEEE INC. NEW YORK., US Seite 1213, Absatz "Recommendations..."	1-17
A	US 5 010 331 A (DIAS DONALD R ET AL) 23 April 1991 (1991-04-23) abstract column 5, line 8 - line 19 column 24, line 1 - line 47 column 33, line 4 - line 12	1
A	PETRIE C S ET AL: "MODELING AND SIMULATION OF OSCILLATOR-BASED RANDOM NUMBER GENERATORS" IEEE INTERNATIONAL SYMPOSIUM ON CIRCUITS AND SYSTEMS (ISCAS),US,NEW YORK, IEEE, 12 May 1996 (1996-05-12), pages 324-327, XP000704602 ISBN: 0-7803-3074-9 paragraph '04.3!; figure 1	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/I 01/00111

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DD 279763 A	13-06-1990	NONE	
US 5010331 A	23-04-1991	US 4935645 A	19-06-1990
		US 4897860 A	30-01-1990
		US 4870401 A	26-09-1989
		US 5838256 A	17-11-1998
		US 4943804 A	24-07-1990

INTERNATIONALER RECHERCHENBERICHT

Internatio s Aktenzeichen
PCT/I _ 01/00111

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F7/58

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	"INTEGRATED CIRCUIT COMPATIBLE RANDOM NUMBER GENERATOR" IBM TECHNICAL DISCLOSURE BULLETIN,US,IBM CORP. NEW YORK, Bd. 30, Nr. 11, 1. April 1988 (1988-04-01), Seiten 333-335, XP000021682 ISSN: 0018-8689 Seite 334, Absatz 2	1-17
Y	DD 279 763 A (THAELMANN SCHWERMASCHBAU VEB) 13. Juni 1990 (1990-06-13) in der Anmeldung erwähnt das ganze Dokument	1-17

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
'A' Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
'E' älteres Dokument, das jedoch erst am oder nach dem Internationalen Anmeldedatum veröffentlicht worden ist
'L' Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
'O' Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
'P' Veröffentlichung, die vor dem Internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

'T' Spätere Veröffentlichung, die nach dem Internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
'X' Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
'Y' Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
'&' Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der Internationalen Recherche	Absendedatum des internationalen Recherchenberichts
18. Juni 2001	04/07/2001

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Cohen, B

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	MURRY: "A General Approach for Generating Natural Random Variables" IEEE TRANSACTIONS ON ELECTRONIC COMPUTERS., Bd. c-19, Nr. 12, Dezember 1970 (1970-12), Seiten 1210-1213, XP002169916 IEEE INC. NEW YORK., US Seite 1213, Absatz "Recommendations..."	1-17
A	US 5 010 331 A (DIAS DONALD R ET AL) 23. April 1991 (1991-04-23) Zusammenfassung Spalte 5, Zeile 8 - Zeile 19 Spalte 24, Zeile 1 - Zeile 47 Spalte 33, Zeile 4 - Zeile 12	1
A	PETRIE C S ET AL: "MODELING AND SIMULATION OF OSCILLATOR-BASED RANDOM NUMBER GENERATORS" IEEE INTERNATIONAL SYMPOSIUM ON CIRCUITS AND SYSTEMS (ISCAS),US,NEW YORK, IEEE, 12. Mai 1996 (1996-05-12), Seiten 324-327, XP000704602 ISBN: 0-7803-3074-9 Absatz '04.3!; Abbildung 1	1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/E_ 91/00111

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
DD 279763	A	13-06-1990	KEINE		
US 5010331	A	23-04-1991	US	4935645 A	19-06-1990
			US	4897860 A	30-01-1990
			US	4870401 A	26-09-1989
			US	5838256 A	17-11-1998
			US	4943804 A	24-07-1990